A complementary construction using mutually unbiased bases

Gaofei Wu and Matthew G. Parker *

December 4, 2013

Abstract

We propose a construction for complementary sets of arrays that exploits a set of mutually-unbiased bases (a MUB). In particular we present, in detail, the construction for complementary pairs that is seeded by a MUB of dimension 2, where we enumerate the arrays and the corresponding set of complementary sequences obtained from the arrays by projection. We also sketch an algorithm to uniquely generate these sequences. The pairwise squared inner-product of members of the sequence set is shown to be $\frac{1}{2}$. Moreover, a subset of the set can be viewed as a codebook that asymptotically achieves $\sqrt{\frac{3}{2}}$ times the Welch bound.

1 Introduction

Sequences with relatively flat Fourier spectra are of central importance for many communications systems such as spread-spectrum, and are also used to probe structures in the context of measurement and detection. It is often the case that a set of such sequences is required, where family members are pairwise distinguishable - in the context of communication each user may be assigned a different sequence from the set, and in the context of measurement the pairwise distinguishability implies that, when probing a structure, each sequence in the set contributes useful information to the overall measurement or detection problem. One recent communication application is to orthogonal frequency-division multiplexing (OFDM), which is a communication technique used in several wireless communication standards such as IEEE 802.16 Mobile WiMAX. A major problem with OFDM is the large peak-to-average power ratio (PAPR) of uncoded OFDM time signals (i.e. the signals do not have relatively flat inverse Fourier spectra). *Complementary sequences* [12, 29, 4] are sets of sequences that have out-of-phase aperiodic autocorrelations that sum to zero. This implies that they have

*G. Wu is with the State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, 710071, China. He is a visiting PhD student (Sep. 2012 – Aug. 2014) in the Department of Informatics, University of Bergen, Norway: gaofei.wu@student.uib.no, M. G. Parker is with the Department of Informatics, University of Bergen, Norway: matthew@ii.uib.no.

very flat Fourier spectra - the Fourier transform of each sequence satisfies a PAPR upper bound of 2.0, which is very low, and Davis and Jedwab [8] showed, in the context of OFDM, how to construct 'standard' 2^h-ary complementary sequences of length 2^n, comprising second-order cosets of generalized first-order Reed-Muller codes $RM_{2^h}(1, n)$. As they are members of $RM_{2^h}(1, n)$, the sequences have good pairwise distinguishability. The work was subsequently extended by [22, 26, 27] and by numerous other authors [31]. [19, 20, 17, 10, 15, 21] show that the complementary set construction is primarily an array construction, where sequence sets are obtained by considering suitable projections of the arrays. It is desirable to propose complementary constructions that significantly improve set size without greatly compromising the upper bound on PAPR or the pairwise distinguishability.

In this paper we show that the problem of construction of large sets of complementary sequences with good pairwise distinguishability is naturally solved by seeding the recursive construction with optimal *mutually-unbiased bases* (MUBs) [28, 14, 24]. By way of example, we construct a set of complementary array pairs over the alphabet $\mathcal{A} = \{0, 1, i, -1, -i\}$ (up to normalisation of the sequence), whose sequence projections can be viewed as a superset of the standard quaternary complementary sequences of [8], where our construction enlarges set size without compromising PAPR or pairwise distinguishability, at the cost of adding '0' to the QPSK alphabet - this construction exploits an optimal MUB of dimension 2. The exact number of arrays that we construct is determined. An algorithm for generating all unique sequence projections from these arrays is then sketched out and an implementation of this algorithm allows us to compute the number of these sequences. These computational results then help us to theoretically establish corresponding enumeration formulae, where we are guided in our theoretical development by related enumerations that we found in the Online Encyclopaedia of Integer Sequences [18]. The construction generates a set of complementary sequences which is a relatively large superset of the complementary sequences obtained in [8], but we show that the magnitude of the pairwise inner product between members of the set remains at $\frac{1}{\sqrt{2}}$, the same as for the set in [8].

This paper can also be seen as a generalisation of the construction in [3], where the authors proposed a family of complementary sequences over $\{0, 1, -1\}$. Moreover the paper can be seen as an explicit consequence of the more general principles for the construction of complementary sets, as described in [21]. There exist related matrix-based approaches to complementary sequence design in the literature. For instance, the complete complementary code approach of [30] and the paraunitary matrix approach to filter banks for complementary sequences, as discussed in [5, 6] - the word 'paraunitary' refers to a matrix polynomial in Z^{-1} that is unitary when $|Z| = 1$, and the approach of these papers is clearly similar to our own. In particular, the recent work in [6] makes extensive recursive use of paraunitary matrices to generate QAM complementary sequence pairs.

A subset of our sequence set can be viewed as a codebook, where the magnitude of the pairwise inner product between codewords in the codebook approaches $\sqrt{\frac{3}{2}}$ times the Welch bound as length increases [32, 25].

After some preliminaries in section 2, we introduce our main construction in section 3. To begin with we develop the complementary construction in a general way, for complementary

sets, so as to emphasise that we can seed with any MUB of any dimension. But, for the general case, it remains open to develop formulae for the size of the array and sequence sets, and for the magnitude of the pairwise inner product between members of the sets. So, for this paper, we only develop in detail the case where we seed our construction with an optimal MUB of dimension 2, i.e. we construct complementary pairs. Nevertheless this is an important case, and it serves to illustrate more general principles. In section 4 we give the exact enumeration of the complementary arrays and sequences we construct, as well as sketch an algorithm to generate the sequences uniquely. The maximum pairwise inner product between sequences in our set is determined in section 5. In section 6, we give our codebook construction. Section 7 concludes with some open problems.

2 Preliminaries

2.1 Mutually unbiased bases

Denote the magnitude of the normalised pairwise inner product of two equal-length complex vectors, u and v, by

$$\Delta(u,v) = \frac{|\langle u,v\rangle|}{|u|\cdot|v|}.$$

A pair of bases $u_0,\cdots,u_{\delta-1}$ and $v_0,\cdots,v_{\delta-1}$ in $\mathbb{C}^\delta$ is said to be *mutually unbiased* if they are both orthonormal and there is a constant a such that $\Delta^2(u_i,v_j) = |\langle u_i,v_j\rangle|^2 = a$, $\forall i,j$. A set of bases is then called a set of mutually unbiased bases (MUB) if any pair of them is mutually unbiased. It is known that a MUB contains at most $\delta+1$ bases in $\mathbb{C}^\delta$, in which case the MUB is referred to as an *optimal* MUB. Such optimal MUBs exist if δ is a prime power [14], in which case $a=\frac{1}{\delta}$. We refer to an optimal MUB as $\mathcal{M}_\delta$ [1] . Specifically, in this paper, we focus on a particular matrix form of $\mathcal{M}_2$, where the 3 bases are the rows of the 3 unitary matrices, I, H, and N, where $I=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, $H=\frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1&1\\1&-1\end{smallmatrix}\right)$, and $N=\frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1&i\\1&-i\end{smallmatrix}\right)$, where $i=\sqrt{-1}$.

The properties of a matrix MUB remain unchanged with respect to row/column reordering and multiplication of a row/column by a unity phase shift, as summarised by the following equivalence relationship between two $S\times S$ unitary complex matrices, M and M':

$$M' = O_\theta P_\theta M P_\gamma O_\gamma,$$

where O_γ and O_θ are diagonal unitary matrices, and P_γ and P_θ are permutation matrices. However there is no distance between two vectors whose elements differ only by a constant phase shift, so to ensure that Δ for our constructed sequence set is nonzero, we force $O_\theta = O_\gamma = I$ and, therefore, only use the equivalence

$$M' = P_\theta M P_\gamma. \tag{1}$$

In this paper we also make use of the Pauli matrices $X=\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ and $Z=\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$.

[1] Up to trivial symmetries and, for a fixed δ, there may be more than one choice of $\mathcal{M}_\delta$.

2.2 Complementary arrays and sequences

Let $F(z) = (F_0(z), F_1(z), \ldots, F_{S-1}(z))^T$ be a length S vector of polynomials, where $F_k(z) = \sum_{i=0}^{d_k-1} F_{k,i} z^i$, $F_{k,i} \in \mathbb{C}$, $\forall i$, is a complex polynomial of degree $d_k - 1$, $0 \leq k < S$. We also associate with and refer to $F_k(z)$ as the length d_k sequence $(F_{k,0}, F_{k,1}, \ldots, F_{k,d_k-1})$. The *aperiodic autocorrelation* of F_k is given by the coefficients of $F_k(z)F_k^*(z^{-1})$, where $*$ means complex conjugate. Let

$$\lambda_F(z) = \langle F(z), F(z) \rangle = F^\dagger(z^{-1})F(z),$$

be the inner-product of F with itself, where $\dagger$ means 'transpose-conjugate' [2] . For $S \geq 2$, we desire to find S degree $d-1$ polynomials, $F_k(z)$, such that $\lambda_F(z) = \lambda_F$, a constant independent of z, in which case the set $\mathcal{F}(z) = \{F_0(z), F_1(z), \ldots, F_{S-1}(z)\}$ is called a size S *complementary set* of length d sequences.

Example: Let $S = 2$, $F_0(z) = 1 + z + z^2 - z^3$, $F_1(z) = 1 + z - z^2 + z^3$. Then $\langle F(z), F(z) \rangle = \lambda_F(z) = (-z^{-3} + z^{-1} + 4 + z - z^3) + (z^{-3} - z^{-1} + 4 - z + z^3) = 8$, so $\mathcal{F}(z) = \{F_0(z), F_1(z)\}$ is a size 2 complementary set of length 4 sequences, where the sequences are $(1, 1, 1, -1)$ and $(1, 1, -1, 1)$.

The complementary set property can be interpreted in the Fourier domain by evaluating z on the unit circle. If $\mathcal{F}$ is a complementary set of size S, then

$$\lambda_F = F^\dagger(\alpha^{-1})F(\alpha), \qquad |\alpha| = 1.$$

It follows that

$$F_k(\alpha)F_k^*(\alpha^{-1}) \leq \lambda_F, \qquad |\alpha| = 1, 0 \leq k < S. \tag{2}$$

(2) states that the Fourier power spectrum of each sequence F_k, $0 \leq k < S$, is upper-bounded by λ_F. If $\|F_k\|^2 = \sum_{0 \leq i < n} F_{k,i}F_{k,i}^* = 1$, $0 \leq k < S$, i.e. if each of the S sequences has its power normalised to 1, then $\lambda_F = S$ and we say that the *peak-to-average power ratio* (PAPR) of each sequence in $\mathcal{F}$ is upper-bounded by S.

We can generalize further by replacing z with $\mathbf{z} = (z_0, z_1, \ldots, z_{n-1})$, where $F_k(\mathbf{z})$ is of degree $d_{k,j} - 1$ in variable z_j, $0 \leq j < n$, in which case $F_k(\mathbf{z})$ is associated with and referred to as an n-dimensional $d_{k,0} \times d_{k,1} \times \ldots d_{k,n-1}$ complex array. The aperiodic autocorrelation of F_k is given by the coefficients of $F_k(\mathbf{z})F_k^*(\mathbf{z}^{-1})$, where $\mathbf{z}^{-1} = (z_0^{-1}, z_1^{-1}, \ldots, z_{n-1}^{-1})$ and, as before, $\mathcal{F}(\mathbf{z})$ is a complementary set of size S if

$$\lambda_F = \lambda_F(\mathbf{z}) = \langle F(\mathbf{z}), F(\mathbf{z}) \rangle = F^\dagger(\mathbf{z}^{-1})F(\mathbf{z}).$$

Example: Let $S = 2$, $F_0(\mathbf{z}) = 1 + z_0 + z_1 - z_0z_1$, $F_1(\mathbf{z}) = 1 + z_0 - z_1 + z_0z_1$. Then $\langle F(\mathbf{z}), F(\mathbf{z}) \rangle = \lambda_F(\mathbf{z}) = (-z_0^{-1}z_1^{-1} + z_0z_1^{-1} + 4 + z_0^{-1}z_1 - z_0z_1) + (z_0^{-1}z_1^{-1} - z_0z_1^{-1} + 4 - z_0^{-1}z_1 + z_0z_1) = 8$, so $\mathcal{F}(\mathbf{z}) = \{F_0(\mathbf{z}), F_1(\mathbf{z})\}$ is a size 2 complementary set of 2×2 arrays, where the arrays are $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right)$.

[2] Comparing $F_k(z)F_k^*(z^{-1})$ with $F^\dagger(z^{-1})F(z)$, we see that, whilst z^{-1} is on the right for the former it is on the left for the latter. This is simply because F is a $S \times 1$ vector - there is no deeper meaning.

Section 3 introduces the construction for complementary sets, i.e. general S, and this construction can be seeded with an optimal MUB, $\mathcal{M}_\delta$, where $\delta = S$. But we subsequently only develop formulae for the case where $\delta = S = 2$ so, for that case, $d_{k,j} = d_j = 2$, $0 \leq j < n$, $\forall k$, and therefore $F_k(\mathbf{z}) \in (\mathbb{C}^2)^{\otimes n}$, i.e. the coefficients of $F_k(\mathbf{z})$ form an array $\in (\mathbb{C}^2)^{\otimes n}$. We shall then recursively construct a set of complementary pairs of arrays, $\mathcal{F}(\mathbf{z})$. The set of distinct complementary arrays obtained from $\mathcal{F}(\mathbf{z})$ is called $\mathcal{B}_n$. Then, by applying projections $z_i = z^{2^{\pi(i)}}$, $0 \leq i < n$, over all permutations, π, in the symmetric group $\mathcal{S}_n$, we shall construct, from $\mathcal{F}(\mathbf{z})$, a set of complementary pairs of sequences, $\mathcal{F}(z)$. The set of complementary sequences obtained from $\mathcal{F}(z)$ is called $\mathcal{B}_{\downarrow,n}$. We shall compute values for $|\mathcal{B}_n|$ and $|\mathcal{B}_{\downarrow,n}|$ in terms of n, and then develop theoretical formulae for these two parameters that agree with our computations. We shall also determine, theoretically, that, when seeded with $\mathcal{M}_2 = \{I, H, N\}$,

$$\Delta^2(\mathcal{B}_{\downarrow,n}) = \max\{\Delta^2(u,v) | u \neq v, u, v \in \mathcal{B}_{\downarrow,n}\} = \frac{1}{2}.$$

Example: The array $F_k(\mathbf{z}) = 1 + z_0 - z_1 + z_0 z_1$ can be projected down to the sequence $F_k(z) = 1 + z - z^2 + z^3$ by the assignment $z_1 = z^2$, $z_0 = z$, and to $F_k(z) = 1 - z + z^2 + z^3$ by the assignment $z_0 = z^2$, $z_1 = z$.

As well as expressing our arrays and sequences as the coefficients of polynomials $F_k(\mathbf{z})$ and $F_k(z)$, respectively, we can, for the case $S = 2$, and where we seed our construction with $\mathcal{M}_2 = \{I, H, N\}$, further express them as generalized Boolean functions, $f_k(\mathbf{x}) : \mathbb{F}_2^n \to \mathcal{A}$, where $\mathcal{A} = \{0, 1, i, -1, -i\}$, $i = \sqrt{-1}$, and $F_k(\mathbf{z}) = c \sum_{\mathbf{x} \in \mathbb{F}_2^n} f_k(\mathbf{x}) \mathbf{z}^{\mathbf{x}}$, where c is some normalising constant, chosen so that the associated array, F_k, satisfies $\|F_k(\mathbf{z})\|^2 = \sum_{0 \leq i < n} F_{k,i} F_{k,i}^* = 1$. When we refer to $f_k(\mathbf{x})$ as an array or sequence, we mean that the 2^n elements of the array or sequence are the 2^n evaluations of $f_k(\mathbf{x})$ for $\mathbf{x} \in \mathbb{F}_2^n$. These elements are also the 2^n coefficients of $F_k(\mathbf{z})$ or $F_k(z)$, respectively. The interpretation of $f_k(\mathbf{x})$ as one of a set of $n!$ sequence projections, depending on $\pi \in \mathcal{S}_n$, as opposed to the parent array, is implicitly made and should be clear from the context of the discussion.

Example: The array $F_k(\mathbf{z}) = c(1 + z_0 + i z_1 z_2 - i z_0 z_1 z_2)$, where $c = \frac{1}{2}$, may be represented by $f_k(\mathbf{x}) = (x_1 + x_2 + 1) i^{2x_0 x_2 + x_2}$, and f_k may also refer, via projection, to one of $3! = 6$ sequences, e.g. with $z_2 = z$, $z_0 = z^2$, $z_1 = z^4$, we project to $F_k(z) = c(1 + z^2 + i z^5 - i z^7)$, which is then one of the 6 sequences represented by f_k [3] .

In section 3, after presenting the general complementary set construction, we explicitly seed the construction with $\mathcal{M}_2 = \{I, H, N\}$ and, thereby, recursively construct a set of complementary arrays, $\mathcal{B}_n$, and project the arrays down to a set of sequences, $\mathcal{B}_{\downarrow,n}$, where the sequence PAPR upper bound of $S = \delta = 2$ follows from the unitarity of I, H, and N, and where the value of $\Delta^2(\mathcal{B}_{\downarrow,n}) = \frac{1}{2}$ follows from the value of Δ for $\mathcal{M}_2$.

[3] More accurately, we should write $f_k(\pi(\mathbf{x}))$ to indicate one of 6 possible permutations but, to reduce notation, we make such a mapping implicit in this paper.

3 The complementary set construction

3.1 The general construction

Let $\mathbf{w} = (w_0, w_1, \ldots, w_{m-1}) \in \mathbb{C}^m$, and $\mathbf{y} = (y_0, y_1, \ldots, y_{m'-1}) \in \mathbb{C}^{m'}$, be disjoint vectors of m and m' complex variables, respectively, and let $\mathbf{z} = \mathbf{w} \cup \mathbf{y} \in \mathbb{C}^{m+m'}$ be the vector of variables formed from the union of variables in $\mathbf{w}$ and $\mathbf{y}$, with some ordering on the variables. Let $F_j(\mathbf{w}) : \mathbb{C}^m \to \mathbb{C}$ be of degree $d_j - 1$ in variable w_j, $0 \leq j < m$. Let $F(\mathbf{w}) = (F_0(\mathbf{w}), F_1(\mathbf{w}), \ldots, F_{S-1}(\mathbf{w}))^T$, and let $\mathcal{U}(\mathbf{y}) = (u_{ij}(\mathbf{y}), 0 \leq i, j < S)$ be an $S \times S$ unnormalised unitary matrix with elements being complex polynomials $u_{ij}(\mathbf{y}) : \mathbb{C}^{m'} \to \mathbb{C}$. By unnormalised unitary we mean that $\mathcal{U}(\mathbf{y})\mathcal{U}^\dagger(\mathbf{y}) = \lambda_{\mathcal{U}}(\mathbf{y})I$, where I is the $S \times S$ identity matrix.

Let $\lambda_F(\mathbf{w}) = \sum_{k=0}^{S-1} F_k(\mathbf{w}) F_k{}^*(\mathbf{w^{-1}})$, and define $F'(\mathbf{z})$ by

$$F'(\mathbf{z}) = \mathcal{U}(\mathbf{y})F(\mathbf{w}). \tag{3}$$

It follows from the unitarity of $\mathcal{U}$, and from (3), that

$$\lambda_{F'}(\mathbf{z}) = \sum_{k=0}^{S-1} F'_k(\mathbf{z}) F'^*_k(\mathbf{z^{-1}}) = \lambda_{\mathcal{U}}(\mathbf{y})\lambda_F(\mathbf{w}). \tag{4}$$

If $\lambda_F(\mathbf{w}) = c_F$, a constant, independent of $\mathbf{w}$, and $\lambda_{\mathcal{U}}(\mathbf{y}) = c_{\mathcal{U}}$, a constant, independent of $\mathbf{y}$ then $\lambda_{F'}(\mathbf{z}) = c_{F'} = c_{\mathcal{U}} c_F$ is a constant, independent of $\mathbf{z}$. If so, then (3) defines a step in the construction of generalised $|\mathbf{z}|$-dimensional complementary array sets of size S from $|\mathbf{w}|$-dimensional complementary array sets of size S, and (4) characterises the complementary property that the sum of the S aperiodic array autocorrelations, $F'_k(\mathbf{z})F'^*_k(\mathbf{z^{-1}})$, is a constant, independent of $\mathbf{z}$. In this paper we only consider the case where $w_i \neq y_j$, $\forall i, j$, but complementarity holds even when this is not true.

Example: Let $F(w) = (1 + w, 1 - w)^T$ and $\mathcal{U}(y) = \begin{pmatrix} 1 & y \\ 1 & -y \end{pmatrix}$. Then $F'(\mathbf{z}) = F'(y, w) = \mathcal{U}(y)F(w) = (1 + w + y - wy, 1 + w - y + wy)^T$. As $\lambda_F(w) = F(w^{-1})^\dagger F(w) = 4$, and $\lambda_{\mathcal{U}}(y) = 2$, then $\lambda_{F'}(z) = 8$. So the arrays comprising the coefficients of $1 + w + y - wy$ and $1 + w - y + wy$ are a complementary set of size $S = 2$, i.e. a complementary pair.

We can recurse (3). With notational changes, the j'th recursive step of (3) is described by,

$$F_j(\mathbf{z}_j) = \mathcal{U}_j(\mathbf{y}_j)F_{j-1}(\mathbf{z}_{j-1}), \tag{5}$$

where $\mathbf{y}_j = (z_{\mu_j}, z_{\mu_j+1}, \ldots, z_{\mu_j+m_j-1})$, $\mathbf{z}_j = (z_0, z_1, \ldots, z_{\mu_j+m_j-1})$, $\mu_j = \sum_{i=0}^{j-1} m_j$, $\mu_0 = 0$, $F_j(\mathbf{z}_j) = (F_{j,0}(\mathbf{z}_j), F_{j,1}(\mathbf{z}_j), \ldots, F_{j,S-1}(\mathbf{z}_j))^T$, and $F_{-1} = \frac{1}{\sqrt{S}}(1, 1, \ldots, 1)$. (5) is a very general recursive equation for the construction of complementary sets of arrays of size S.

We argue, in this paper, that it is natural, for (5), to choose $\mathcal{U}_j$ from a MUB, $\mathcal{M}_\delta$, where $\delta = S$, at each stage of the recursion. More precisely, we seed with $\mathcal{U}_j(\mathbf{y}_j)$ where $\mathcal{U}_j$ is taken from $\mathcal{M}_\delta$, and the variables, $\mathbf{y}_j$, are introduced via another matrix. This is made clear in the next subsection. The complementary properties, (i.e. PAPR $\leq S = \delta$) are guaranteed

because every member of $\mathcal{M}_\delta$ is a unitary matrix. Moreover, the pairwise inner-product between arrays or sequences generated will be small because Δ is minimised for $\mathcal{M}_\delta$. At the same time, the size of the sequence set is maximised because we can choose $\mathcal{U}_j$ to be one of $\delta+1$ unitaries (for δ a prime power). Finally the size of the projected sequence set can be further increased by choosing one of $\delta!$ permutations of the rows of the unitaries at each stage of the recursion.

For general $S=\delta$ it remains open to develop theoretical formulae for the size of our constructed array and sequence sets, and for the Δ value for the sets. But we do solve these issues for the special case where $S=\delta=2$, and this is the topic of the rest of this paper. Note, however, that our choice of $\mathcal{M}_2$ allows us express things in terms of generalised Boolean functions, and this facilitates our theoretical development. It is likely that such functional methods do not, in general, extend to $S=\delta>2$.

3.2 Seeding with $\mathcal{M}_2$ to generate complementary pairs

We now consider the special case where $\mathcal{U}_j$ is selected from $\mathcal{M}_2=\{I,H,N\}$ at each stage of the recursion, i.e. we focus on the case where $\delta=S=2$, and generate complementary pairs. Moreover we let $m_j=1$, $\forall j$, so $\mu_j=j$ and $\mathcal{U}_j(\mathbf{y}_j)=\mathcal{U}_j(z_j)$, $\forall j$.

From (5), let $F'_j(\mathbf{z}_j)=\mathcal{U}'_j(z_j)F'_{j-1}(\mathbf{z}_{j-1})$ where, using the equivalence of (1), we set $\mathcal{U}'_j(z_j)=P_{\theta_{j+1}}\mathcal{U}_j(z_j)P_{\gamma_j}$. Let $F_j(\mathbf{z}_j)=P^{-1}_{\theta_{j+1}}F'_j(\mathbf{z}_j)$. Then

$$F_j(\mathbf{z}_j)=\mathcal{U}_j(z_j)P_{\gamma_j}P_{\theta_j}F_{j-1}(\mathbf{z}_{j-1}).$$

Without loss of generality we simplify $P_{\gamma_j}P_{\theta_j}$ to P_j, and obtain

$$F_j(\mathbf{z}_j)=\mathcal{U}_j(z_j)P_jF_{j-1}(\mathbf{z}_{j-1}).$$

We now separate $\mathcal{U}_j(z_j)$ into MUB and variable parts:

$$\mathcal{U}_j(z_j)=\mathcal{U}_jP_{\mathcal{U}_j}V_j(z_j),$$

where $P_{\mathcal{U}_j}$ is a permutation unitary (the diagonal unitary, $O_{\mathcal{U}_j}$, is set to I for the reason given in subsection 2.1), $V_j(z_j)=\left(\begin{smallmatrix}1&0\\0&z_j\end{smallmatrix}\right)$ and $\mathcal{U}_j\in\mathcal{M}_2$. So

$$F_j(\mathbf{z}_j)=\mathcal{U}_jP_{\mathcal{U}_j}V_j(z_j)P_jF_{j-1}(\mathbf{z}_{j-1}).$$

As $P_{\mathcal{U}_j}\in\{I,X\}$, $HX=ZH$, and $NX=iZXN$, we swap $\mathcal{U}_j$ and $P_{\mathcal{U}_j}$, replace $P_{j+1}P_{\mathcal{U}_j}$ by P_j, and obtain

$$F_j(\mathbf{z}_j)=P_j\mathcal{U}_jV_j(z_j)F_{j-1}(\mathbf{z}_{j-1}), \tag{6}$$

where $P_j\in\{I,X\}$. (We ignore global constants such as '$i=\sqrt{-1}$' as they have no effect on our final construction).

Let $\mathcal{U} = (\mathcal{U}_0, \mathcal{U}_1, \ldots, \mathcal{U}_{n-1}) \in \mathcal{M}_2^n$. Then we recurse (6) n times so as to construct

$$F_{n-1}(\mathbf{z}) = \begin{pmatrix} F_{n-1,0}(\mathbf{z}) \\ F_{n-1,1}(\mathbf{z}) \end{pmatrix}, \quad \text{where } F_{n-1,k}(\mathbf{z}) = c \sum_{\mathbf{x} \in \mathbb{F}_2^n} f_{n-1,k}(\mathbf{x}) \mathbf{z}^{\mathbf{x}}, \qquad k \in \{0,1\}, \tag{7}$$

$\mathbf{z}^{\mathbf{x}} = \prod_{j=0}^{n-1} z_j^{x_j}$, and c is some real constant such that $F_{n-1,k}(\mathbf{z})$ is normalised as an array (sum of element square-magnitudes is 1). It remains to characterise $f_{n-1,k}$.

To begin with, let $\mathcal{U}_j = H$ and $P_j = I$, $\forall j$. Then we construct

$$f_{n-1,k}(\mathbf{x}) : \mathbb{F}_2^n \to \{1, -1\} = i^{2(kx_{n-1} + \sum_{j=0}^{n-2} x_j x_{j+1})}.$$

These are binary complementary sequences, as constructed in [8]. This function is illustrated by (1) in Fig 1, and is given by

$$\mathcal{U} = (H, H, H, H) \Rightarrow f_{3,0}(\mathbf{x}) = i^{2(x_0 x_1 + x_1 x_2 + x_2 x_3)}.$$

More generally, let $\mathcal{U}_j \in \{H, N\}$ and let $l = (j, \mathcal{U}_j = N)$. Then we construct

$$f_{n-1,k}(\mathbf{x}) : \mathbb{F}_2^n \to \{1, i, -1, -i\} = i^{2(kx_{n-1} + \sum_{j=0}^{n-2} x_j x_{j+1}) + \sum_{j=0}^{|l|-1} x_{l(j)}}.$$

These are quaternary complementary sequences, as constructed in [8]. An example of this function for $l = (1, 3)$ is illustrated by (2) in Fig 1, and is given by

$$\mathcal{U} = (H, N, H, N) \Rightarrow f_{3,0}(\mathbf{x}) = i^{2(x_0 x_1 + x_1 x_2 + x_2 x_3) + x_1 + x_3}.$$

More generally, let $\mathcal{U}_j \in \mathcal{M}_2 = \{I, H, N\}$, where $\mathcal{U}_{n-1} \neq I$, and let $p = (j, \mathcal{U}_j \in \{H, N\})$, $s = (j, \mathcal{U}_j = I)$ and let $q(v) = j$ if $\mathcal{U}_j \neq I$ and $\mathcal{U}_i = I$, $\forall i$, $v < i < j$, $j < n$, $j \neq v$, and let $q(v) = n$ otherwise. Then we construct

$$f_{n-1,k}(\mathbf{x}) : \mathbb{F}_2^n \to \mathcal{A} = \Big(\prod_{j=0}^{|s|-1} (x_{s(j)} + x_{q(s(j))} + 1)\Big) i^{2(kx_{p(|p|-1)} + \sum_{j=0}^{|p|-2} x_{p(j)} x_{p(j+1)}) + \sum_{j=0}^{|l|-1} x_{l(j)}},$$

where $p(-1) = n$, $x_n = 0$, and $\mathcal{A} = \{0, 1, i, -1, -i\}$. An example of this function for $p = (0, 3, 5)$, $l = (3, 5)$, $s = (1, 2, 4)$, and $q = (3, 3, 3, 5, 5, 6)$, is illustrated by (3) in Fig 1, and is given by

$$\mathcal{U} = (H, I, I, N, I, N) \Rightarrow f_{5,0}(\mathbf{x}) = (x_1 + x_3 + 1)(x_2 + x_3 + 1)(x_4 + x_5 + 1) i^{2(x_0 x_3 + x_3 x_5) + x_3 + x_5}.$$

More generally, let $\mathcal{U}_j \in \mathcal{M}_2 = \{I, H, N\}$. Moreover, if, for some t, $\mathcal{U}_{n-1} = \mathcal{U}_{n-2} = \cdots = \mathcal{U}_{n-t} = I$, $0 \leq t \leq n$, and $\mathcal{U}_{n-t-1} \neq I$, then define b such that $b(j) = 1$ for $j \geq n - t$, and $b(j) = 0$ otherwise. Then we construct (8). An example of this function for $p = (0, 2)$,

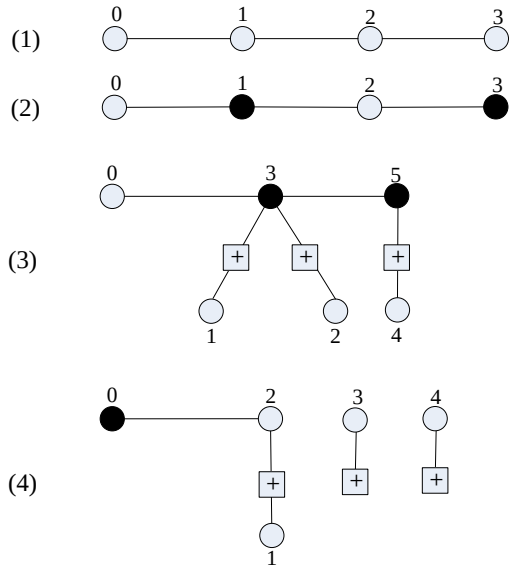

Figure 1: Graph Representations of Example Functions

$l = (0)$, $s = (1, 3, 4)$, $q = (2, 2, 5, 5, 5)$, and $b = (0, 0, 0, 1, 1)$, is illustrated by (4) in Fig 1, and is given by

$$\mathcal{U} = (N, I, H, I, I) \Rightarrow f_{4,k}(\mathbf{x}) = (x_1 + x_2 + 1)(x_3 + k + 1)(x_4 + k + 1)i^{2(kx_2 + x_0x_2) + x_0}.$$

We summarise the previous discussion with the following definition.

Definition 1 *Let $p = (j, \mathcal{U}_j \in \{H, N\})$, $l = (j, \mathcal{U}_j = N)$, and $s = (j, \mathcal{U}_j = I)$ be vectors of integers ordered by magnitude. Let $q(v) = j$ if $\mathcal{U}_j \neq I$ and $\mathcal{U}_i = I$, $\forall i$, $v < i < j$, $j < n$, $j \neq v$, and let $q(v) = n$ otherwise. If, for some t, $\mathcal{U}_{n-1} = \mathcal{U}_{n-2} = \cdots = \mathcal{U}_{n-t} = I$, $0 \leq t \leq n$, and $\mathcal{U}_{n-t-1} \neq I$, then define b such that $b(j) = 1$ for $j \geq n - t$, and $b(j) = 0$ otherwise.*

Then we can construct (7), where

$$f_{n-1,k}(\mathbf{x}) : \mathbb{F}_2^n \rightarrow \mathcal{A} = \Big(\prod_{j=0}^{|s|-1} (x_{s(j)} + x_{q(s(j))} + kb(s(j)) + 1)\Big) i^{2\left(kx_{p(|p|-1)} + \sum_{j=0}^{|p|-2} x_{p(j)}x_{p(j+1)}\right) + \sum_{j=0}^{|l|-1} x_{l(j)}}, \tag{8}$$

where $p_{-1} = n$, $x_n = 0$, and $\mathcal{A} = \{0, 1, i, -1, -i\}$.

The graphical language of Fig 1 generalises the path graph of [8, 22] whilst, at the same time, making a precise mathematical connection with factor graph notation [16], and to quantum graph states [13] and their generalisations [23].

As mentioned previously, we interpret the coefficients of $F_{n-1,k}(\mathbf{z})$ as an array in $(\mathbb{C}^2)^{\otimes n}$, i.e. an n-dimensional $2 \times 2 \times \ldots \times 2$ complex array. However, from (7), $F_{n-1,k}(\mathbf{z})$ is wholly

dependent on $f_{n-1,k}(\mathbf{x})$ and, in the following, much of the exposition will be developed in terms of f rather than F, so we also refer to f as an array, where the array elements are the 2^n evaluations of f at $\mathbf{x} \in \mathbb{F}_2^n$. The subsequent projections of F, from array to sequence, then carry over to f in an obvious way.

In (8), we have, for ease of exposition, set $P_j = I$, $\forall j$. More generally, let $r = (r(0), r(1), \ldots, r(n-1)) \in \mathbb{F}_2^n$ be such that $P_j = X^{r(j)}$, $\forall j$. Moreover, let
$w = (w(0), w(1), \ldots, w(n-1)) \in \mathbb{F}_2^n$, where

$$w(i) = \sum_{i}^{q(i)-1} r(i).$$

Our later enumerations multiply by 2^n to take into account that $r \in \mathbb{F}_2^n$, and this multiplicity carries over to w as the mapping from $r \rightarrow w$ is one-to-one. We then generalise (8) to:

$$\begin{aligned} f_{n-1,k}(\mathbf{x}) : \mathbb{F}_2^n \rightarrow \mathcal{A} = \\ (\textstyle\prod_{j=0}^{|s|-1}(x_{s(j)} + x_{q(s(j))} + kb(s(j)) + w(s(j)) + 1)) \times \\ i^{2(kx_{p(|p|-1)} + \sum_{j=0}^{|p|-1} w(p(j))x_{p(j)} + \sum_{j=0}^{|p|-2} x_{p(j)}x_{p(j+1)}) + \sum_{j=0}^{|l|-1} x_{l(j)}}, \end{aligned} \tag{9}$$

From (9), the set of complementary arrays is $\mathcal{B}_n = \{f_{n-1,0}(\mathbf{x}) | \mathcal{U} \in \mathcal{M}_2^n, r \in F_2^n\}$. In the next section we evaluate $|\mathcal{B}_n|$ where, evidently, $|\mathcal{B}_n| \leq 6^n$.

The arrays constructed in Theorem 1 of [3] are a subset of those described by (9), corresponding to the case where $\mathcal{U} \in \{I, H\}^n$, with $t = 0$. [3, Conjecture 1] can, consequently, be improved to

Conjecture 1 *For any n, each type-I complementary array over the alphabet $\{0, 1, -1\}$ is of the form*

$$f_{n-1,0}(\mathbf{x}) \;\; = (\prod_{j=0}^{|s|-1}(x_{s(j)} + x_{q(s(j))} + w(s(j)) + 1))(-1)^{\sum_{j=0}^{|p|-1} w(p(j))x_{p(j)} + \sum_{j=0}^{|p|-2} x_{p(j)}x_{p(j+1)}}. \tag{10}$$

('Type-I' complementarity is just the form of complementarity discussed in this paper for arrays over $(\mathbb{C}^2)^{\otimes n}$).

4 Enumerations

In this section we evaluate $|\mathcal{B}_n|$. We also evaluate $|\mathcal{B}_{\downarrow,n}|$, which is the number of complementary sequences of length 2^n that can be obtained from arrays in $\mathcal{B}_n$ by the projections, $z_i = z^{2^{\pi(i)}}$, $\pi \in \mathcal{S}_n$, from the n-dimensional arrays down to 1 dimensional sequences of length 2^n. Clearly there are an infinite number of other projections one could choose, e.g. $z_i = z^{3^{\pi(i)}}$, $\pi \in \mathcal{S}_n$, and for which complementarity would be preserved, but we do not consider such variations in this paper.

4.1 Number of arrays in $\mathcal{B}_n$

We associate $\mathcal{U}$ with a length n binary sequence $a = (a_0, a_1, \cdots, a_{n-1})$, where 0 represents I and 1 represents H or N. Let

$$\mathcal{B'}_n = \{\mathcal{B}_n | \mathcal{U}_{n-1} \neq I\}.$$

Theorem 1

$$|\mathcal{B'}_n| = \begin{cases} 2^n \cdot \sum_{k=0}^{n-1} (\binom{n-1}{k} 2^{n-k-1} + \binom{\frac{n}{2}-1}{\lfloor \frac{k}{2} \rfloor} \cdot 2^{\lceil \frac{n-k}{2} \rceil - 1}) = 2^n \cdot 3^{n-1} + 2^{n+1} \cdot 3^{\frac{n}{2}-1}, \text{ for } n \text{ even}, \\ 2^n \cdot \sum_{k=0}^{n-1} (\binom{n-1}{k} 2^{n-k-1} + \binom{\frac{n-1}{2}}{\frac{k}{2}} \cdot 2^{\lceil \frac{n-k}{2} \rceil - 1}) = 2^n \cdot 3^{n-1} + 2^n \cdot 3^{\frac{n-1}{2}}, \text{ for } n \text{ odd}, \end{cases} \tag{11}$$

where $\binom{n}{t} = 0$, *if* t *is not an integer.*

Proof. There are $\binom{n-1}{k}$ binary sequences of length $n-1$ with k zeros. Let $\binom{n-1}{k} = S_k + A_k$, where S_k (or A_k) is the number of symmetric (or asymmetric) length $n-1$ binary sequences with k zeros. We have that

$$S_k = \begin{cases} \binom{\frac{n-1}{2}}{\frac{k}{2}}, \text{ for } n-1 \text{ even}, \\ \binom{\lfloor \frac{n-1}{2} \rfloor}{\lfloor \frac{k}{2} \rfloor}, \text{ for } n-1 \text{ odd}. \end{cases}$$

Let $2^{n-k} = S'_k + A'_k$, where S'_k (or A'_k) is the number of symmetric (or asymmetric) binary sequences of length $n-k$. Note that $S'_k = 2^{\lceil \frac{n-k}{2} \rceil}$ and $a_{n-1} = 1$. Let a have k zeros. Then, when $(a_0, a_1, \cdots, a_{n-2})$ is symmetric, there are $S'_k + \frac{A'_k}{2} = \frac{2S'_k + A'_k}{2} = \frac{2^{n-k} + S'_k}{2}$ choices for the $n-k$ $1's$ to be H or N. When $(a_0, a_1, \cdots, a_{n-2})$ is asymmetric there are 2^{n-k} choices for the $n-k$ $1's$ to be H or N. Then

$$\begin{aligned} |\mathcal{B'}_n| &= 2^n \cdot \sum_{k=0}^{n-1} (S_k \cdot \frac{2^{n-k} + S'_k}{2} + \frac{N_k}{2} \cdot 2^{n-k}) \\ &= 2^n \cdot \sum_{k=0}^{n-1} ((S_k + N_k) \cdot \frac{2^{n-k}}{2} + \frac{S_k}{2} \cdot S'_k) \\ &= 2^n \cdot \sum_{k=0}^{n-1} (\binom{n-1}{k} \cdot 2^{n-k-1} + \frac{S_k}{2} \cdot S'_k) \\ &= \begin{cases} 2^n \cdot \sum_{k=0}^{n-1} (\binom{n-1}{k} 2^{n-k-1} + \binom{\frac{n}{2}-1}{\lfloor \frac{k}{2} \rfloor} \cdot 2^{\lceil \frac{n-k}{2} \rceil - 1}), \text{ for } n \text{ even}, \\ 2^n \cdot \sum_{k=0}^{n-1} (\binom{n-1}{k} 2^{n-k-1} + \binom{\frac{n-1}{2}}{\frac{k}{2}} \cdot 2^{\lceil \frac{n-k}{2} \rceil - 1}), \text{ for } n \text{ odd}, \end{cases} \end{aligned} \tag{12}$$

□

Corollary 1 *The number of arrays in* $\mathcal{B}_n$ *is*

$$\begin{aligned} |\mathcal{B}_n| &= \sum_{m=0}^{n} |\mathcal{B'}_m| \cdot 2^{n-m} \\ &= \begin{cases} 2^{n-1} \cdot (3^n + 3 \cdot 3^{\frac{n}{2}} - 2), \ \textit{for } n \textit{ even}, \\ 2^{n-1} \cdot (3^n + 5 \cdot 3^{\frac{n-1}{2}} - 2), \ \textit{for } n \textit{ odd}, \end{cases} \end{aligned} \tag{13}$$

where $|\mathcal{B'}_0| = 1$.

In [8] the authors construct the set of standard quaternary complementary sequences, $\mathcal{DJ}_n$, being $\mathbb{Z}_4$-linear offsets of the $\mathbb{F}_2$ 'path graph' [22]. Using our terminology this translates to the construction of (9) under the restriction $\mathcal{U} \in \{H, N\}^n$, i.e. where $|s| = 0$. Although [8] only viewed their objects as complementary sequences they are, more generally, complementary arrays over $(\mathbb{C}^2)^{\otimes n}$ [19, 20, 17, 15, 10, 21]. As n gets large, $|\mathcal{B}_n|$ approaches 6^n, whereas the size of the construction of [8] approaches 4^n. The larger size of our set is achieved by enlarging the alphabet from $\{1, i, -1, -i\}$ in [8] to $\{0, 1, i, -1, -i\}$ in this paper, more accurately, by selecting our unitaries from $\mathcal{M}_2 = \{I, H, N\}$ instead of from the sub-optimal MUB $\{H, N\}$. (A sub-optimal MUB is a set of mutually unbiased bases where the number of bases is less than the maximum possible. When δ is a prime power, then the maximum possible number of bases is $\delta + 1$ and, for $\mathcal{M}_2$, $\delta + 1 = 3$.) But, crucially, as discussed later, the increase in set size for the set of sequence projections is achieved without any increase in Δ, i.e. $\Delta(\mathcal{B}_{\downarrow,n}) = \Delta(\mathcal{DJ}_n)$.

4.2 An algorithm for generating all sequences in $\mathcal{B}_{\downarrow,n}$, and the corresponding enumeration

Many practical applications of our construction would exploit the length 2^n sequences obtained from the arrays in $\mathcal{B}_n$ by projection. Such sequences comprise the set $\mathcal{B}_{\downarrow,n}$. By projection we mean the following. We have that $F_{n-1,0}(\mathbf{z}) = c \sum_{\mathbf{x} \in \mathbb{F}_2^n} f_{n-1,0}(\mathbf{x}) \mathbf{z}^{\mathbf{x}}$, for $f_{n-1,0}$ as defined in (9). The coefficients of this polynomial form an n-dimensional array, and can be projected down to a 1-dimensional array by the assignments $z_j = z^{2^j}$. Such a projection produces a polynomial in z of degree $2^n - 1$ whose coefficients form a length 2^n sequence with elements from $\mathcal{A} = \{0, 1, i, -1, -i\}$. More generally, for each $F_{n-1,0}(\mathbf{z})$, we generate the $n!$ projections obtained by assigning $z_j = z^{2^{\pi(j)}}$, $\forall \pi \in \mathcal{S}_n$, where $\mathcal{S}_n$ is the group of permutations of n objects. These projections can be obtained by generating $\mathcal{B}_{\downarrow,n} = \{f_{n-1,0}(\mathbf{x}_\pi), \forall \mathcal{U} \in \mathcal{M}_2^n, r \in \mathbb{F}_2^n, \forall \pi \in \mathcal{S}_n\}$, where $\mathbf{x}_\pi = (x_{\pi(0)}, x_{\pi(1)}, \ldots, x_{\pi(n-1)})$. Not all these projections are unique when taken over all polynomials in $\mathcal{B}_n$. We sketch out, in a stepwise fashion, a recursive algorithm that generates sequences in $\mathcal{B}_{\downarrow,n}$ uniquely, firstly when $\mathcal{U} \in \{I, H\}^n$, and then for $\mathcal{U} \in \mathcal{M}_2^n$. In each case we implemented the algorithm, obtained computational results, and then proved the results. It should be noted that the theoretical developments were greatly helped by us first plugging our computational results into the On-Line Encyclopedia of Integer Sequences (OEIS) [18].

We refer to $\mathcal{U} \in \{I, H\}^n$ as an 'IH string' and $\mathcal{U} \in \mathcal{M}_2^n$ as an 'IHN string'. Moreover we abbreviate vectors, e.g. (I, H, I, H, H) is shortened to $IHIHH$, and (N, H, H, I, N, I) to $NHHINI$, and abbreviate $f_{n-1,0}(\mathbf{x})$ to $f(\mathbf{x})$ or f.

4.2.1 An algorithm for $\mathcal{U} \in \{I, H\}^n$

We set $P_j = I$, $\forall j$, and choose $\mathcal{U} \in \{I, H\}^n$. It is possible that two IH strings generate the same sequence, so we must consider three uniqueness criteria, as follows.

Criterion A: Consider, as an example, that we generate the sequence associated with $\mathcal{U} = HIIHIHII$, i.e. we generate $f = (x_1 + x_3 + 1)(x_2 + x_3 + 1)(x_4 + x_5 + 1)(x_6 + 1)(x_7 + 1)(-1)^{x_0x_3+x_3x_5}$. The projection down to a sequence depends on the ordering, π, of the 8 variables in $\mathbf{x}$, i.e. $\pi(\mathbf{x}) = (x_{\pi(0)}, x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, x_{\pi(4)}, x_{\pi(5)}, x_{\pi(6)}, x_{\pi(7)})$, $\pi \in \mathcal{S}_8$. The number of sequences generated in this way is 8!.

The form of f implies that $x_1 = x_2 = x_3$ and $x_4 = x_5$. Moreover x_6 and x_7 can be swapped without changing the function. So permuting 1, 2, and 3, and/or swapping 4 and 5, and/or swapping 6 and 7, has no effect on the function, and reduces the function enumeration to $\frac{8!}{3!2!2!}$. In order to avoid these repetitions we only allow $\pi \in \mathcal{S}_8$ under the conditions $\pi(1) < \pi(2) < \pi(3)$, $\pi(4) < \pi(5)$, and $\pi(6) < \pi(7)$.

Criterion B: Consider the sequence generated by $IHIIHHII$. This generates $f' = (x_0 + x_1 + 1)(x_2 + x_4 + 1)(x_3 + x_4 + 1)(x_6 + 1)(x_7 + 1)(-1)^{x_1x_4+x_4x_5}$. For the example of f discussed for criterion A, $f(\pi(\mathbf{x})) = f'(\mathbf{x})$ for some $\pi \in \mathcal{S}_8$. This is because $IHIIH$ is the reversal of $HIIHI$. So, to ensure unique generation, only one of f or f' should be generated. Ignoring the rightmost HII, one can interpret the IH strings, $HIIHIHII$ and $IHIIHHII$, as binary strings 10010 and 01001, respectively. With the least significant bit on the left, we equate these strings with integers 9 and 18, respectively, and throw away, arbitrarily, the IH string associated with the largest number, namely $IHIIHHII$.

Criterion C: The symmetry of criterion B does not occur if the IH substring is symmetric under reversal. For instance, consider the string $IHHIHI$. Then, ignoring the rightmost HI, we see that $IHHI$ is symmetric. So there is no f' to throw away. However, this symmetric condition leads, instead, to an alternative restriction on the allowed permutation π. For instance, for this example, we allow only one of the permutations (354120) and (124350), (which are both valid under previous conditions on π) as they both lead to $f = (x_1 + x_2 + 1)(x_3 + x_5 + 1)(x_0 + 1)(-1)^{x_2x_4+x_4x_5}$. Ignoring all integers to the right of the position of the rightmost H, i.e. in this case ignoring '0', we choose, arbitrarily, to throw away the permutation with the lowest integer on the right-hand side - in this case we throw away (354120) as '1' is on the right-hand side of (35412). One needs to refine this decision process. Consider the string $IHIHIHI$, and permutations (4602351) and (3502461), which are both valid under previous conditions on π. We see that $IHIHI$ is symmetric. Then, ignoring '1', the lowest integer, '0', is in the centre of (460235), as $x_0 = x_2$, so we choose to decide between the two permutations on the next lowest off-centre integer. In this case, we decided based on integer '3' and throw away (4602351) as '3' is right of centre in this permutation.

n	1	2	3	4	5	6	7	8	9	10
$E_{IH}(n)$	2	5	17	83	557	4715	47357	545963	7087517	102248075
$\tilde{E}_{IH}(n)$	2	6	26	150	1082	9366	94586	1091670	14174522	204495126
$\log_2(E_{IH}(n))$	1	2.32	4.09	6.38	9.12	12.20	15.53	19.06	22.76	26.61
$\log_2(\frac{n!}{2})$	0	0	1.58	3.58	5.91	8.49	11.30	14.30	17.47	20.79

Table 1: $E_{IH}(n) = \#\text{Unique } IH \text{ Sequences}, P_j = I, \forall j$ - A032262[18]

We have implemented a recursive algorithm based on criteria A, B, and C, and obtain the enumerations shown in Table 4.2.1. Let us call this number $E_{IH}(n)$. We show that $E_{IH}(n)$ is sequence A032262 of [18].

We make use of the following combinatoric numbers:

Stirling's number of the second kind:
$$S_2(n,k) = \left\{ \begin{array}{c} n \\ k \end{array} \right\} = \tfrac{1}{k!}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^n.$$

generalized ordered Bell numbers:
$$B(r,n) = r\sum_{k=1}^{n}\binom{n}{k}B(r,n-k) = \sum_{k=0}^{n} r^k k! \left\{ \begin{array}{c} n \\ k \end{array} \right\}, \qquad B(r,0) = 1. \tag{14}$$

$B(r,n)$ is A094416 of [18]. The case when $r = 1$ generates the ordered Bell numbers.

Theorem 2 *The enumeration of IH strings of length n, taking into account criteria A, B, and C, is given by*
$$E_{IH}(n) = 2^{n-1} + \sum_{k=0}^{n} k! \left\{ \begin{array}{c} n \\ k \end{array} \right\}.$$

Proof. (of theorem 2) We first enumerate $\tilde{E}_{IH}(n)$, which only takes criterion A into account. Ignoring criteria B and C causes a double count of unique IH strings except for $III\ldots I, HII\ldots I, IHI\ldots I, IIH\ldots I, \ldots, III\ldots H$, i.e. the exceptions are all IH strings of H weight less than 2, for which neither the symmetry of criterion B or of C is possible. These exceptions contribute an additive correction factor of 2^n to $\tilde{E}_{IH}(n)$. We, thereby, obtain a relationship between $E_{IH}(n)$ and $\tilde{E}_{IH}(n)$:
$$\tilde{E}_{IH}(n) = 2E_{IH}(n) - 2^n. \tag{15}$$

We show that $\tilde{E}_{IH}(n)$ is A000629 of [18], and include $\tilde{E}_{IH}(n)$ in table 4.2.1.

Theorem 3 *The enumeration of IH strings, based only on criterion A, is given by*
$$\tilde{E}_{IH}(n) = 2B(1,n), \qquad n > 0, \qquad \tilde{E}_{IH}(0) = 1.$$

Proof. (of theorem 3) Consider all IH strings of length $n-1$ of the form $\ldots H$, i.e. with a rightmost H. Taking into account only criterion A, then let us say that there are $B(n-1)$ unique strings of this type. Let s_{n-1} be any such IH string of length $n-1$. Now consider all IH strings of length n of the form $s_{n-1}I = \ldots HI$, i.e. with a rightmost HI. Considering all variable index permutations, $\pi \in \mathcal{S}_n$, the single rightmost I can be associated with one of n indices. So there are $\binom{n}{1}B(n-1)$ unique strings of the form $s_{n-1}I = \ldots HI$. More generally, consider all IH strings of length $n-k$ of the form $\ldots H$. There are $B(n-k)$ unique strings of this type. Let s_{n-k} be any such IH string of length $n-k$, and consider all IH strings of length n of the form $s_{n-k}II\ldots I = \ldots HII\ldots I$, i.e. with k rightmost I's. Considering all variable index permutations, $\pi \in \mathcal{S}_n$, the k rightmost Is can be associated with $\binom{n}{k}$ indices. So there are $\binom{n}{k}B(n-k)$ unique strings of the form $s_{n-k}II\ldots I$, i.e. with k rightmost Is. With initial conditions $B(0) = 1$, we have that the number of unique IH strings of length n and with at least one rightmost I, taking into account only criterion A, is given by

$$B'(n) = \sum_{k=1}^{n} \binom{n}{k} B(n-k), \qquad B(0) = 1. \tag{16}$$

We are left with enumerating the number, $B(n)$, of unique IH strings with a rightmost H, taking into account only criterion A. We find that

$$B(n) = B'(n). \tag{17}$$

Proof. (of (17)) Let $s_n = vH$ and $t_n = vI$ be two IH strings of length n with a rightmost H and I, respectively, and where v is an IH string of length $n-1$. Let v have r rightmost Is. Then, using criterion A, permutation of the rightmost $r+1$ indices of s_n is a symmetry. Similarly, permutation of the rightmost $r+1$ indices of t_n is also a symmetry. It follows that the enumeration for IH strings with a rightmost H is identical to that for IH strings with a rightmost I. □

Theorem 3 follows from (16) and (17). □

Combining (14), for $r = 1$, with theorem 3 and (15) yields theorem 2. □

An asymptotic formula for $E_{IH}(n)$ can be derived from known results on the asymptote of ordered Bell numbers [1, 33] and A000670 of [18]:

$$E_{IH}(n)_{n\to\infty} = \frac{n!}{2}\log_2(e)^{n+1}. \tag{18}$$

In table 4.2.1 we also compare $\log_2(E_{IH})$ with $\log_2$ of the number of binary standard Golay sequences, where $P_j = I$, $\forall j$ (i.e. ignoring linear offsets).

4.2.2 The IHN strings

Having sketched out an algorithm to generate all sequences uniquely from IH strings, and derived associated enumeration formulae, we now extend to IHN strings. Consider

n	1	2	3	4	5	6	7	8	9
$E_{IHN}(n)$	3	11	63	563	6783	99971	1724943	34031603	755385183
$\tilde{E}_{IHN}(n)$	3	15	111	1095	13503	199815	3449631	68062695	1510769343
$\log_2(E_{IHN}(n))$	1.58	3.46	5.98	9.14	12.73	16.61	20.72	25.02	29.49
$\log_2(n!2^{n-1})$	0	2	4.58	7.58	10.91	14.49	18.30	22.30	26.47

Table 2: $E_{IHN}(n) = \#$Unique IHN Sequences, $P_j = I$, $\forall j$

$HIIHIHII$. If we now include the possibility of N then, once we have generated $HIIHIHII$, along with a specified permutation, we must also generate $NIIHIHII$, $HIINIHII$, $NIINIHII$, $HIIHINII$, $NIIHINII$, $HIININII$, and $NIININII$, i.e. 8 IHN strings in total, all with the same permutation. Criteria A, B, and C have already been tackled in generating the initial IH string, so need not be re-considered.

We have extended our recursive algorithm to IHN strings, and obtain the enumerations shown in Table 4.2.2. Let us call this number $E_{IHN}(n)$, where $|\mathcal{B}_{\downarrow,n}| = 2^n E_{IHN}(n)$. The 2^n factor occurs because we must, more generally, consider $P_j \in \{I, X\}$, $\forall j$.

Theorem 4 *The enumeration of IHN strings of length n, taking into account criteria A, B, and C, is given by*

$$E_{IHN} = 3\sum_{k=0}^{n} 2^{k-2} k! \left\{ \begin{array}{c} n \\ k \end{array} \right\} + 2^n - \frac{1}{2}.$$

Proof. (of theorem 4) We first enumerate $\tilde{E}_{IHN}(n)$, which only takes criterion A into account. Ignoring criteria B and C causes a double count of unique IHN strings except those with H or N of weight less than 2, which contribute an additive correction factor of $2^{n+1} - 1$ to $\tilde{E}_{IHN}(n)$. We, thereby, obtain a relationship between $E_{IHN}(n)$ and $\tilde{E}_{IHN}(n)$:

$$\tilde{E}_{IHN}(n) = 2E_{IHN}(n) - 2^{n+1} + 1. \tag{19}$$

We show that $\tilde{E}_{IHN}(n)$ is A201339 of [18], and include $\tilde{E}_{IHN}(n)$ in table 4.2.2.

Theorem 5 *The enumeration of IHN strings, based only on criterion A, is given by*

$$\tilde{E}_{IHN}(n) = \frac{3}{2}B(2, n), \qquad n > 0, \qquad \tilde{E}_{IHN}(0) = 1.$$

Proof. (of theorem 5) Let $R \in \{H, N\}$. Consider all IHN strings of length $n-k$ of the form $\ldots R$. Taking into account criterion A, let us say that there are $C(n-k)$ unique strings of this type. Let s_{n-k} be any such IHN string of length $n-k$, and consider all IHN strings of length n of the form $s_{n-k}II\ldots I = \ldots RII\ldots I$, i.e. with k rightmost I's.

Considering all variable index permutations, $\pi \in \mathcal{S}_n$, the k rightmost Is can be associated with $\binom{n}{k}$ indices. So there are $\binom{n}{k}C(n-k)$ unique strings of the form $s_{n-k}II\ldots I$, i.e. with k rightmost Is. With initial conditions $C(0)=1$, we have that the number of unique IHN strings of length n and with at least one rightmost I, taking into account only criterion A, is given by

$$C'(n) = \sum_{k=1}^{n} \binom{n}{k} C(n-k), \qquad C(0)=1. \tag{20}$$

We are left with enumerating the number, $C(n)$, of unique IHN strings with a rightmost H or N, taking into account only criterion A. We find that

$$C(n) = 2C'(n). \tag{21}$$

Proof. (of (21)) Let $s_n = vR$ and $t_n = vI$ be two IHN strings of length n with a rightmost H or N, and I, respectively, and where v is an IHN string of length $n-1$. Let v have r rightmost Is. Then, using criterion A, permutation of the rightmost $r+1$ indices of s_n is a symmetry. Similarly, permutation of the rightmost $r+1$ indices of t_n is also a symmetry, irrespective of whether the rightmost element is H or N. It follows that the enumeration for IHN strings with a rightmost H or N is exactly twice that for IH strings with a rightmost I. □

Theorem 5 follows from (20), (21), and (14). □

Combining (14), for $r=2$, with theorem 5 and (19) yields theorem 4. □

An asymptotic formula for $E_{IHN}(n)$ can be derived from known results on the asymptote for $B(2,n)$ [7]:

$$E_{IHN}(n)_{n\to\infty} = \frac{n!}{4\ln(\frac{3}{2})^{n+1}}. \tag{22}$$

In table 4.2.2 we also compare $\log_2(E_{IHN})$ with $\log_2$ of the number of $\mathbb{Z}_4$ standard Golay sequences, where $P_j = I$, $\forall j$ (i.e. ignoring linear offsets).

4.2.3 The IHN strings plus binary linear offsets

Once we have generated the IHN strings uniquely, the more general choice of $P_j \in \{I, X\}$, $\forall j$, replaces $E_{IHN}(n)$ with $|\mathcal{B}_{\downarrow,n}| = 2^n E_{IHN}(n)$, so all values in table 4.2.2 are multiplied by 2^n (n is added to all log values).

5 Pairwise inner-product

In this section we consider $\Delta^2(\mathcal{B}_{\downarrow,n})$, where

$$\Delta^2(\mathcal{B}_{\downarrow,n}) = \max\{\Delta^2(f,f') | f \neq f', f, f' \in \mathcal{B}_{\downarrow,n}\}.$$

It is worth re-iterating that each f represents one of $n!$ sequences, obtained from each $F(\mathbf{z}) = c\sum_{\mathbf{x}} f(\mathbf{x})\mathbf{z}^{\mathbf{x}}$ by projection to $F(z)$, where the sequence, F, is formed from the coefficients of $F(z)$. Moreover the normalising constant, c, is chosen so that $\|F\|^2 = \sum_{0\le i<n} F_i F_i^* = 1$ (see (9) for more details).

Theorem 6 $\Delta^2(\mathcal{B}_{\downarrow,n}) = \frac{1}{2}$.

Proof. Let $f, f' \in \mathcal{B}_{\downarrow,n}$. Assume that f and f' have 2^{n-e} and $2^{n-e'}$ elements which are not zero, respectively. Then $h = f \cdot f'$ has 2^{n-u} elements which are not zero, where $\max\{e, e'\} \le u \le e + e'$. We obtain the bound

$$\Delta^2(f, f') \le \frac{(2^{n-u})^2}{2^{n-e}2^{n-e'}} = 2^{e+e'-2u}. \tag{23}$$

There are three cases, where the bound of (23) suffices for cases 2 and 3.

Case 1: $e = e'$, and f, f' have the same positions that are non-zero. Let $\widehat{f}$ and $\widehat{f'}$ be the compressed length 2^{n-e} sequences obtained by deleting the zeros in f and f', respectively. Let $\widehat{f} = i^{\tilde{f}}, \widehat{f'} = i^{\tilde{f'}}$, where $\tilde{f}, \tilde{f}' : \mathbb{F}_2^{n-e} \to \mathbb{Z}_4$ are generalized Boolean functions. If the linear terms of $\tilde{f}$ and $\tilde{f}'$ are the same, then the Hamming distance between $\tilde{f}$ and $\tilde{f}'$ is at least 2^{n-e-2}, and $2^{n-e-2} \le N_2 \le 3 \cdot 2^{n-e-2}$, $2^{n-e-2} \le N_0 \le 3 \cdot 2^{n-e-2}$, $N_1 = N_3 = 0$, where

$$N_j = |\{\mathbf{x} | \tilde{f}(\mathbf{x}) - \tilde{f}'(\mathbf{x}) = j, \mathbf{x} \in F_2^{n-e}\}|, \quad j \in \mathbb{Z}_4.$$

Then

$$|\langle f, f'\rangle|^2 = |\sum_{\mathbf{x}\in F_2^{n-e}} i^{\tilde{f}(\mathbf{x})-\tilde{f}'(\mathbf{x})}|^2 = |N_2 - N_0|^2 + |N_3 - N_1|^2 \le |2^{n-e-1}|^2,$$

and

$$\Delta^2(f, f') = \frac{|\langle f, f'\rangle|^2}{2^{n-e} \cdot 2^{n-e}} \le \frac{|2^{n-e-1}|^2}{2^{n-e} \cdot 2^{n-e}} = \frac{1}{4}.$$

If the linear terms of $\tilde{f}$ and $\tilde{f}'$ are different then, since $(\tilde{f} - \tilde{f}') \bmod 2$ is a balanced Boolean function over $\mathbb{Z}_2$, then $N_0 + N_2 = N_1 + N_3 = 2^{n-e-1}$. Then

$$|\langle f, f'\rangle|^2 = |\sum_{\mathbf{x}\in F_2^{n-e}} i^{\tilde{f}(\mathbf{x})-\tilde{f}'(\mathbf{x})}|^2 = |N_2 - N_0|^2 + |N_3 - N_1|^2 \le 2 \cdot |2^{n-e-1}|^2,$$

$$\Delta^2(f, f') = \frac{|\langle f, f'\rangle|^2}{2^{n-e} \cdot 2^{n-e}} \le \frac{2 \cdot |2^{n-e-1}|^2}{2^{n-e} \cdot 2^{n-e}} = \frac{1}{2}.$$

Case 2: $e = e'$, but the non-zero positions of f and f' are different. Then $e + 1 \le u$ and, from (23),

$$\Delta^2(f, f') \le \frac{1}{4}.$$

Case 3: $e \ne e'$. Wlog assume $e < e'$. Then $e' \le u$, and, from (23),

$$\Delta^2(f, f') \le \frac{1}{2}.$$

It remains to exhibit a pair of sequences $a, a' \in \mathcal{B}_{\downarrow,n}$ satisfying $\Delta^2(a, a') = \frac{1}{2}$. For example, $a = (-1)^{\sum_{i=0}^{n-2} x_i x_{i+1}}, a' = a \cdot i^{x_{n-1}}$. □

For the set, $\mathcal{DJ}_n$, of standard quaternary Golay sequences, $\Delta^2(\mathcal{DJ}_n) = \frac{1}{2}$, because $\mathcal{DJ}_n \subset \mathcal{B}_{\downarrow,n}$ and $a, a' \in \mathcal{DJ}_n$.

6 A codebook from a subset of $\mathcal{B}_{\downarrow,n}$

In this section we give a construction for a codebook, $\mathcal{C}$, over $\mathcal{A}$ that is a subset of $\mathcal{B}_{\downarrow,n}$. The maximum magnitude of inner products between distinct codewords is approximately $\sqrt{\frac{3}{2}}$ times the Welch bound for large n.

An $(\mathcal{N}, \mathcal{K})$ codebook, $\mathcal{C} = \{\mathbf{c}_0, \mathbf{c}_1, \cdots, \mathbf{c}_{\mathcal{N}-1}\}$, is a set of $\mathcal{N}$ distinct codewords in a $\mathcal{K}$-dimensional vector space where $\mathcal{K} \leq \mathcal{N}$. Each code vector $\mathbf{c}_h = (c_{h,0}, c_{h,1}, \cdots, c_{h,\mathcal{K}-1}), 0 \leq h < \mathcal{N}$, has unit-norm, i.e., $\|\mathbf{c}_h\| = \sqrt{\sum_{i=0}^{\mathcal{K}-1} |c_{h,i}|^2} = 1$. Welch [32] gave a well-known lower bound on $\Delta(\mathcal{C})$:

$$\Delta(\mathcal{C}) = \max_{0 \leq h \neq m < \mathcal{N}} |\mathbf{c}_h \mathbf{c}_m^\dagger| \geq \Delta_{welch}(\mathcal{C}) = \sqrt{\frac{\mathcal{N} - \mathcal{K}}{\mathcal{K}(\mathcal{N} - 1)}}.$$

If $\Delta(\mathcal{C}) = \Delta_{welch}(\mathcal{C})$, then $\mathcal{C}$ is called a maximum-Welch-bound-equality (MWBE) codebook.

Abbreviate $f_{n-1,0}(\mathbf{x})$ by f, let $f = f_{\mathcal{U}}$ for some fixed $\mathcal{U} \in \mathcal{M}_2^n$, and construct the codeset

$$\mathcal{C}_{\mathcal{U}} = \{f_{\mathcal{U}} \mid r \in \mathbb{F}_2^n\}.$$

Then $\mathcal{C}_{\mathcal{U}}$ comprises 2^n pairwise orthogonal sequences.

Let $\mathcal{R} = \{\mathcal{R}_0, \mathcal{R}_1, \mathcal{R}_2\}$, $\mathcal{R}_j = (\mathcal{R}_{j,0}, \mathcal{R}_{j,1}, \ldots, \mathcal{R}_{j,n-1}) \in \mathcal{M}_2^n$, $0 \leq j \leq 2$, such that

$$\mathcal{R}_{1,i} = I \text{ iff } \mathcal{R}_{0,i} \neq I, \qquad 0 \leq i < n. \tag{24}$$

Let p_j, $j \in \{0, 1\}$, be the vector, p, as defined in Definition 1, for $\mathcal{U} = \mathcal{R}_j$, with border conditions $p_0(-1) = p_1(-1) = -1$. We also require auxiliary vectors $u = \mathcal{R}_0 \cdot \mathcal{R}_1 \in \{H, N\}^n$ and $w \in \mathbb{Z}^n$. We construct w and $\mathcal{R}_2$ element-by-element, i.e. w_i then $\mathcal{R}_{2,i}$ then w_{i+1} then $\mathcal{R}_{2,i+1}$, etc, starting with $w_{p_j(i_j)} = w_0$, where

$$\begin{array}{rll} w_{p_j(i_j)} = |\{h & \mid & \mathcal{R}_{2,p_j(i_j-1)+h} = N, \quad 0 < h < p_j(i_j) - p_j(i_j - 1)\}|, \quad 0 \leq i_j < |p_j|, j \in \{0, 1\}, \\ \mathcal{R}_{2,i} & = H & \text{iff } (w_i \text{ odd }, u(i) = H) \text{ or } (w_i \text{ even }, u(i) = N), \\ & = N & \text{otherwise.} \end{array} \tag{25}$$

For instance, if $\mathcal{R}_0 = (I, I, N, I, I, H, I, I)$ and $\mathcal{R}_1 = (H, N, I, H, H, I, N, N)$ then $p_0 =$

$(2,5)$, $p_1 = (0,1,3,4,6,7)$, and $u = (H,N,N,H,H,H,N,N)$. Then

$$\begin{array}{llll}
w_{p_1(0)} = w_0 = |\{h & | \ \mathcal{R}_{2,p_1(0-1)+h} = N, & 0 < h < 0-(-1) = 1\}| = 0 & \mathcal{R}_{2,0} = N \\
w_{p_1(1)} = w_1 = |\{h & | \ \mathcal{R}_{2,p_1(1-1)+h} = N, & 0 < h < 1-0 = 1\}| = 0 & \mathcal{R}_{2,1} = H \\
w_{p_0(0)} = w_2 = |\{h & | \ \mathcal{R}_{2,p_0(0-1)+h} = N, & 0 < h < 2-(-1) = 3\}| = 1 & \mathcal{R}_{2,2} = N \\
w_{p_1(2)} = w_3 = |\{h & | \ \mathcal{R}_{2,p_1(2-1)+h} = N, & 0 < h < 3-1 = 2\}| = 1 & \mathcal{R}_{2,3} = H \\
w_{p_1(3)} = w_4 = |\{h & | \ \mathcal{R}_{2,p_1(3-1)+h} = N, & 0 < h < 4-3 = 1\}| = 0 & \mathcal{R}_{2,4} = N \\
w_{p_0(1)} = w_5 = |\{h & | \ \mathcal{R}_{2,p_0(1-1)+h} = N, & 0 < h < 5-2 = 3\}| = 1 & \mathcal{R}_{2,5} = H \\
w_{p_1(4)} = w_6 = |\{h & | \ \mathcal{R}_{2,p_1(4-1)+h} = N, & 0 < h < 6-4 = 2\}| = 0 & \mathcal{R}_{2,6} = H \\
w_{p_1(5)} = w_7 = |\{h & | \ \mathcal{R}_{2,p_1(5-1)+h} = N, & 0 < h < 7-6 = 1\}| = 0 & \mathcal{R}_{2,7} = H.
\end{array}$$

So $w = (0,0,1,1,0,1,0,0)$ and $\mathcal{R}_2 = (N,H,N,H,N,H,H,H)$. As another example, if $\mathcal{R}_0 = (H,I,I,I,N)$ and $\mathcal{R}_1 = (I,H,H,H,I)$ then $p_0 = (0,4)$, $p_1 = (1,2,3)$, $u = (H,H,H,H,N)$. Then $w = (0,1,0,0,3)$, and $\mathcal{R}_2 = (N,N,N,N,N)$.

The codebook, $\mathcal{C}$, is then constructed as

$$\mathcal{C} = \mathcal{C}_{\mathcal{R}_0} \cup \mathcal{C}_{\mathcal{R}_1} \cup \mathcal{C}_{\mathcal{R}_2} = \{f_{\mathcal{U}} \mid \mathcal{U} \in \mathcal{R}, r \in \mathbb{F}_2^n\}. \tag{26}$$

$\mathcal{C}$ is actually a codebook of arrays $\in (\mathcal{C}^2)^{\otimes n}$, being $\subset \mathcal{B}_n$, but we further view $\mathcal{C}$ as a codebook of sequences $\subset \mathcal{B}_{\downarrow,n}$ by subsequent projections, as discussed previously.

Theorem 7 *$\mathcal{C}$, as constructed in (26), is a $(3 \times 2^n, 2^n)$ codebook, where $\Delta(\mathcal{C}) = \sqrt{2^{-n}}$, $\Delta_{welch}(\mathcal{C}) = \sqrt{\frac{1}{3.2^n-1}}$, $\Delta(\mathcal{C}) \to \sqrt{\frac{3}{2}}\Delta_{welch}(\mathcal{C})$, as $n \to \infty$.*

Proof. Let p_j, s_j, l_j, and r_j be the vectors p, s, l, r, respectively, for $\mathcal{U} = \mathcal{R}_j$, as defined in Definition 1. (24) implies that $f_{\mathcal{R}_0}$ and $f_{\mathcal{R}_1}$ are both nonzero at only one element, for any $r_0, r_1 \in \mathbb{F}_2^n$. Moreover $\|f_{\mathcal{R}_j}\| = \sqrt{2^{n-|p_j|}}$, and $p_0 + p_1 = n$. It follows that $\Delta(f_{\mathcal{R}_0}, f_{\mathcal{R}_1}) = \sqrt{2^{-n}}$. For $\Delta(f_{\mathcal{R}_0}, f_{\mathcal{R}_2})$ and $\Delta(f_{\mathcal{R}_1}, f_{\mathcal{R}_2})$ we require the following identity:

For any $a \in \mathbb{F}_2^n$,

$$|\sum_{x \in \mathbb{F}_2^n} i^{2a \cdot x + b \cdot x}|^2 = 2^n, \qquad b = (1,1,\ldots,1)^T. \tag{27}$$

Proof. (of (27)) is straightforward and is omitted. □

From (9), $f_{n-1,0}$ can be written as

$$f_{n-1,0}(\mathbf{x}) = \chi(\mathbf{x}) i^{\mathcal{P}(\mathbf{x})},$$

where $\chi(\mathbf{x}) \in \mathbb{F}_2^n$ is a product of linear constraints, and $\mathcal{P}(\mathbf{x}) = 2\mathcal{Q}(\mathbf{x}) + \mathcal{L}(\mathbf{x})$ is the sum of a binary quadratic term, $\mathcal{Q}$, and a $\mathbb{Z}_4$-linear term, $\mathcal{L}$. Let $f_{\mathcal{R}_j} = \chi_j(\mathbf{x}) i^{\mathcal{P}_j(\mathbf{x})}$, where $\mathcal{P}_j = 2\mathcal{Q}_j + \mathcal{L}_j$.

To prove for $\Delta(f_{\mathcal{R}_0}, f_{\mathcal{R}_2})$ we first set $r_0 = r_2 = 0$. Then

$$\begin{aligned}
f_{\mathcal{R}_0} f_{\mathcal{R}_2} &= \chi_0(\mathbf{x}) i^{\mathcal{P}_0(\mathbf{x})} \chi_2(\mathbf{x}) i^{\mathcal{P}_2(\mathbf{x})} = \chi_0(\mathbf{x}) i^{\mathcal{P}_0(\mathbf{x})} i^{\mathcal{P}_2(\mathbf{x})} \qquad (\text{as } \chi_2 = 1) \\
&= \chi_0(\mathbf{x}) i^{\mathcal{P}_0(\mathbf{x})} \chi_0(\mathbf{x}) i^{\mathcal{P}_2(\mathbf{x})} \\
&= \chi_0(\mathbf{x}) i^{2\mathcal{Q}_0(\mathbf{x}) + \mathcal{L}_0(\mathbf{x})} i^{2(\mathcal{Q}_0(\mathbf{x}) + \mathcal{L}'(\mathbf{x})) + \mathcal{L}_2(\mathbf{x})} \qquad \text{for some binary linear } L' \\
&\qquad\qquad (\text{as } \chi_0 \text{ restricts } \mathcal{Q}_2 \text{ to } \mathcal{Q}_0 + \mathcal{L}') \\
&= \chi_0(\mathbf{x}) i^{2\mathcal{L}'(\mathbf{x}) + \mathcal{L}_0(\mathbf{x}) + \mathcal{L}_2(\mathbf{x})}.
\end{aligned} \tag{28}$$

The key point in (28) is that the quadratic terms, $\mathcal{Q}_0$, cancel. χ_0 equates subsets of the variables in $\mathbf{x}$ as follows:

$$y_i = x_{p_0(i-1)+1} = x_{p_0(i-1)+2} = \ldots = x_{p_0(i)}, \qquad 0 \leq i < |p_0|. \tag{29}$$

We re-express (28) as

$$f_{\mathcal{R}_0} f_{\mathcal{R}_2} = i^{2\mathcal{L}'(\mathbf{y})+\mathcal{L}_0(\mathbf{y})+\mathcal{L}_2(\mathbf{y})}, \qquad \mathbf{y} \in \mathbb{F}_2^{|p_0|}.$$

Then

$$\langle f_{\mathcal{R}_0}, f_{\mathcal{R}_2} \rangle = \sum_{\mathbf{y} \in \mathbb{F}_2^{|p_0|}} i^{2\mathcal{L}'(\mathbf{y})+\mathcal{L}_0(\mathbf{y})+\mathcal{L}_2(\mathbf{y})}.$$

It follows, using (27), that $|\langle f_{\mathcal{R}_0}, f_{\mathcal{R}_2} \rangle|^2 = 2^{|p_0|}$ iff

$$\mathcal{L}_0(\mathbf{y}) + \mathcal{L}_2(\mathbf{y}) = 2\mathcal{L}''(\mathbf{y}) + \mathbf{1} \cdot \mathbf{y}, \tag{30}$$

for some binary linear term, $\mathcal{L}''$. Our construction satisfies (30) because the conditions of (25) on $\mathcal{R}_2$ ensure the contribution of an odd number of N terms for each y_i, i.e. the addition of an odd number of $\mathbb{Z}_4$ linear terms, y_i, $\forall i$, $0 \leq i < |p_0|$, giving y_i or $3y_i = 2y_i + y_i$, where $2y_i$ contributes to $\mathcal{L}''$. It follows that $\Delta^2(f_{\mathcal{R}_0}, f_{\mathcal{R}_2}) = \frac{|\langle f_{\mathcal{R}_0}, f_{\mathcal{R}_2} \rangle|^2}{2^{|p_0|}2^n} = 2^{-n}$.

The generalisation to any $r_0, r_1 \in F_2^n$ simply adds more binary linear terms to $\mathcal{L}'$ in (28) and/or changes $x_{p_0(i-1)+h}$ to $x_{p_0(i-1)+h} + 1$ for one or more h. Neither modification affects the result.

The proof for $\Delta(f_{\mathcal{R}_1}, f_{\mathcal{R}_2})$ is identical to that for $\Delta(f_{\mathcal{R}_0}, f_{\mathcal{R}_2})$. □

Lemma 1 *There are $2^{n-1}(2^n - 1)$ distinct codebooks, $\mathcal{C} \in \mathcal{B}_n$, of arrays that can be generated by (26).*

Proof. (sketch) There are 2^n ways to share out the I's between $\mathcal{R}_0$ and $\mathcal{R}_1$. For each one of these, there are 2^n choices for $\{H, N\}^n$. But $\mathcal{R}_0$ and $\mathcal{R}_1$ could be swapped so, to avoid this symmetry, set the first element of $\mathcal{R}_0$ equal to I, which halves our count so we get 2^{2n-1}. However this includes the possibility that $\mathcal{R}_0 = (I, I, I, \ldots, I)$, in which case $\mathcal{R}_1, \mathcal{R}_2 \in \{H, N\}^n$ and there is a double count as $\mathcal{R}_1$ and $\mathcal{R}_2$ could be swapped, so we must subtract 2^{n-1} from 2^{2n-1}. □

We leave open the problem of enumerating the number of distinct codebooks, $\mathcal{C} \in \mathcal{B}_{\downarrow,n}$, of sequences, as generated by (26).

We can further construct a codebook that is a subset of $\mathcal{C}$ and that approaches $\sqrt{2}\Delta_{welch}$ for large n, as follows.

Let $\mathcal{R} = \{\mathcal{R}_0, \mathcal{R}_1\}$, $\mathcal{R}_j \in \{I, H\}^n$, $0 \leq j \leq 1$, and let

$$\mathcal{C}^{IH} = \{f_{\mathcal{U}} \mid \mathcal{U} \in \mathcal{R}, r \in \mathbb{F}_2^n\}, \tag{31}$$

under the condition

$$\mathcal{R}_{1,i} = I \text{ iff } \mathcal{R}_{0,i} \neq I, \qquad 0 \leq i < n.$$

Theorem 8 *$\mathcal{C}^{IH}$ is a $(2^{n+1}, 2^n)$ codebook, where $\Delta(\mathcal{C}^{IH}) \to \sqrt{2}\Delta_{welch}(\mathcal{C}^{IH})$, as $n \to \infty$.*

Proof. Omitted - a simple subcase of the previous construction. □

By mapping $I \to 0$, $N \to 1$, $H \to 2$, one can interpret $\mathcal{R}$ as a code over $\mathbb{F}_3$, i.e. a ternary code. For instance, one choice of $\mathcal{R}$ is $\{II\ldots I, NN\ldots N, HH\ldots H\}$ which can be interpreted as the ternary repetition code $\{00\ldots0, 11\ldots1, 22\ldots2\}$ so, in a sense, we are constructing a codebook from a ternary code. It would be interesting, in future work, to construct codebooks from other, larger, ternary codes, both linear and nonlinear.

In [2] a codebook that asymptotes to $\sqrt{6}$ times the Welch bound is constructed. It is interesting because of the way it is constructed from complementary sequences, and is motivated, in particular, by application to compressed sensing. However, unlike $\mathcal{B}_{\downarrow,n}$, the codebook members are not designed to satisfy an upper bound on PAPR, so the codebook of [2] is not comparable in this sense to $\mathcal{B}_{\downarrow,n}$.

7 Conclusion

We have described a construction for complementary sets of arrays and sequences using a recursive matrix notation, and then proposed to seed the construction with an optimal MUB. Specifically, we focused on the $\mathcal{M}_2$ case to construct complementary pairs. Thereby, we constructed a set, $\mathcal{B}_n$, of complementary arrays over $(\mathbb{C}^2)^{\otimes n}$, and have projected $\mathcal{B}_n$ down to a set, $\mathcal{B}_{\downarrow,n}$, of length 2^n complementary sequences that is a superset of the quaternary set of standard complementary sequences, $\mathcal{DJ}_n$, constructed in [8]. Whilst $|\mathcal{B}_{\downarrow,n}|$ is significantly larger than $|\mathcal{DJ}_n|$, the PAPR upper bound remains at 2, and the magnitude of the pairwise inner-product between set members remains at $\frac{1}{\sqrt{2}}$, i.e. $\Delta(\mathcal{B}_{\downarrow,n}) = \Delta(\mathcal{DJ}_n)$.

Unlike most constructions for QAM complementary sequences in the literature, the sequences in $\mathcal{B}_{\downarrow,n}$ all possess the same power, i.e. $\|F, F\|^2 = 1$, $\forall F \in \mathcal{B}_{\downarrow,n}$. So the upper bound on PAPR for the sequence carries over to the upper bound on PAPR for the set. The QAM constructions in the literature typically propose sets of sequences with varying powers - this could be a disadvantage in some applications. This 'equal power' property for $\mathcal{B}_{\downarrow,n}$ would carry over to complementary constructions using more general $\mathcal{M}_\delta$. However, this 'equal power' property also has a downside when $\mathcal{M}_2$ is used. For example, consider the size 2^n subset of $\mathcal{B}_{\downarrow,n}$ sequences constructed using $\mathcal{U} = (I, I, I, \ldots, I)$, $r \in \mathbb{F}_2^n$. These are 2^n spikes or pulses of very large relative magnitude and, in some contexts, it may be practically undesirable to generate such sequences. So, in some contexts, one might choose to generate the subset of $\mathcal{B}_{\downarrow,n}$, generated from $\mathcal{U} \in \mathcal{M}_2^{\otimes n}$, where the number of I's in $\mathcal{U}$ is not too big.

We also extracted a codebook from $\mathcal{B}_{\downarrow,n}$ that achieves $\sqrt{\frac{3}{2}}$ times the Welch bound for large n. It is of interest because every member of the codebook also satisfies PAPR ≤ 2.

The primary aim of this paper is to advertise the central role played by the optimal MUB in our construction. Although the method is applicable to an optimal MUB of any dimension, we focused on $\mathcal{M}_2 = \{I, H, N\}$, of dimension $\delta = 2$, so as to recursively construct

the complementary sequence set, $\mathcal{B}_{\downarrow,n}$. The parameters of $\mathcal{M}_2$ control the parameters of $\mathcal{B}_{\downarrow,n}$ in that the sequences of $\mathcal{B}_{\downarrow,n}$ satisfy a PAPR upper-bound of $\delta = 2$ precisely because I, H, and N are $\delta \times \delta$ unitary, the value of $|\mathcal{B}_{\downarrow,n}|$ is large because $|\mathcal{M}_2| = 3 = \delta + 1$, the maximum value possible, and the value of $\Delta(\mathcal{B}_{\downarrow,n})$ is small because $\Delta = \frac{1}{\delta} = \frac{1}{2}$ for $\mathcal{M}_2$ is the minimum possible.

7.1 Some open problems

When δ is a prime power then we know that $|\mathcal{M}_\delta| = \delta + 1$. If, in (5), we assign the non-variable part of $\{\mathcal{U}_j(\mathbf{y}_j)\}$ to $\mathcal{M}_\delta$ then we generalise the results of this paper to $\delta \geq 2$. One expects the complementary set of arrays, $\mathcal{B}_{\mathcal{M}_\delta,n}$, and sequences, $\mathcal{B}_{\mathcal{M}_\delta,\downarrow,n}$, constructed from the recursion of (5), to have very good properties. We know that the PAPR for $\mathcal{B}_{\mathcal{M}_\delta,n}$ and $\mathcal{B}_{\mathcal{M}_\delta,\downarrow,n}$, is upper-bounded by δ, but

- Can one develop expressions for $|\mathcal{B}_{\mathcal{M}_\delta,n}|$ and $|\mathcal{B}_{\mathcal{M}_\delta,\downarrow,n}|$ in terms of just δ and n?
- Can one develop expressions for $\Delta(\mathcal{B}_{\mathcal{M}_\delta,\downarrow,n})$ in terms of just δ and n?

The use of $\mathcal{M}_2$ in our construction ensures that our arrays and sequences have elements drawn from the alphabet $\{0, 1, i, -1, -i\}$ (up to normalisation), and this facilitates our development of expressions for $|\mathcal{B}_{\downarrow,n}|$ and $\Delta(\mathcal{B}_{\downarrow,n})$. There exist similar optimal Fourier-based MUBs, $\mathcal{M}_\delta$, for δ a prime power, where the functional approach used in this paper seems to generalise naturally. But not all optimal MUBs are of this form so, for general MUBs, we propose the following challenge:

- Design an algorithm for the receiver, based on the matrix alphabet, $\mathcal{M}_\delta$, to decode received sequences that have been generated at the transmitter using the complementary construction seeded by $\mathcal{M}_\delta$.

In section 6, we suggest that it is somewhat natural to map from the ternary alphabet $\{0, 1, 2\}$ to $\mathcal{M}_2 = \{I, N, H\}$. Thus 'strong' codes over $\{0, 1, 2\}$ might be used to select relatively strong subsets of $\mathcal{B}_n$ and $\mathcal{B}_{\downarrow,n}$. It would be interesting to investigate, not just the ternary case, but more general mappings from codes over $\{0, 1, \ldots, \delta\}$ to subsets of the complementary array/sequence sets that have been seeded using $\mathcal{M}_\delta$.

We constructed a codebook that meets $\sqrt{\frac{3}{2}}$ times the Welch bound as $n \to \infty$. Although the codebook does not meet the Welch bound with equality, it does have the extra rather strict constraint that every sequence in the set satisfies PAPR ≤ 2. This extra constraint is well-motivated for, for instance, spread-spectrum applications, and suggests the following challenge:

- We wish to find an infinite construction for a codebook, $\mathcal{C}$, where every sequence in $\mathcal{C}$ satisfies PAPR $\leq T$. Then how close can $\mathcal{C}$ get to the Welch bound? One expects that the answer depends on T. The problem also clearly depends on the relative sizes of $\mathcal{K}$ and $\mathcal{N}$. For instance, let $\mathcal{C}$ be the subset of $\mathcal{B}_{\downarrow,n}$ where $\mathcal{U} = (H, H, \ldots, H)$ and

$r \in \mathbb{F}_2^n$. Then $\mathcal{N} = |\mathcal{C}| = 2^n$, $\mathcal{K} = 2^n$, so the Welch bound is 0 and is met with equality by $\mathcal{C}$ as the sequences in $\mathcal{C}$ are pairwise orthogonal. Moreover $\mathrm{PAPR}(\mathcal{C}) \leq 2$. So the interesting cases occur for $\mathcal{K} > \mathcal{N}$.

Finally, we have focused on recursive complementary constructions seeded by optimal MUBs such as $\mathcal{M}_2$. More generally, it would be interesting to seed our construction with other unitary matrix sets that are not necessarily MUBs. Moreover, we could even seed with sets of non-unitary matrices, in which case we could obtain larger sets at the price of PAPR rising with n, and larger Δ. For instance, it would be interesting to seed with the single $\delta^2 \times \delta$ matrix whose δ^2 rows comprise an equiangular tight frame of dimension δ, where Δ for the frame is $\frac{1}{\delta+1}$.

Acknowledgement: We wish to thank the reviewers for their helpful comments on the paper.

References

[1] J. P. Barthelemy, "An asymptotic equivalent for the number of total preorders on a finite set", *Discrete Mathematics*, 29(3):311–313, 1980.

[2] X. Bian, N. Y. Yu, "Partial Fourier Codebooks Associated with Multiplied Golay Complementary Sequences for Compressed Sensing", *Sequences and Their Applications* - SETA 2012 Lecture Notes in Computer Science Volume 7280, pp 257–268, 2012.

[3] T. E. Bjørstad, M. G. Parker, "Equivalence Between Certain Complementary Pairs of Types I and III", in Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. Invited talk at NATO Science for Peace and Security Series - D: Information and Communication Security, 23, Edited by: B. Preneel, S. Dodunekov, V. Rijmen and S. Nikova, June 2009. `http://www.ii.uib.no/~matthew/CompEquivCorrected.pdf`

[4] S. Z. Budǐsin, "New complementary pairs of sequences", *Electron. Lett.*, 26:881–883, 1990.

[5] S. Z. Budǐsin, P. Spasojević, "Filter Bank Representation of Complementary Sequence Pairs", Fiftieth Annual Allerton Conference, Allerton House, UIUC, Illinois, USA, October 1–5, 2012.

[6] S. Z. Budǐsin, P. Spasojević, "Paraunitary generation/correlation of QAM complementary sequence pairs", *Cryptography and Communications*, 5(3), September, 2013.

[7] B. Cloitre, The On-Line Encyclopedia of Integer Sequences, A050351 (A094416), asymptotic formula, `http://oeis.org/`, 2013.

[8] J. A. Davis and J. Jedwab, "Peak-to-mean power control for OFDM, Golay complementary sequences, and Reed-Muller codes", *IEEE Trans. Inform. Theory*, vol. 45, no. 11, pp. 2397–2417, Nov. 1999.

[9] T. Durt, B-G. Englert, I. Bengtsson, K. Zyczkowski, "On mutually unbiased bases", *Int. J. Quantum Information*, 8, 535–640, 2010. arXiv:1004.3348v2 [quant-ph].

[10] F. Fiedler, J. Jedwab, M. G. Parker, "A Multi-dimensional Approach to the Construction and Enumeration of Golay Complementary Sequences", *J. Combinatorial Theory (Series A)*, vol. 115 pp. 753–776, 2008.

[11] F. Fiedler, J. Jedwab, and M. G. Parker, "A framework for the construction of Golay sequences," *IEEE Trans. Inform. Theory*, vol. 54, no. 7, pp. 3113-3129, Jul. 2008.

[12] M. J. E. Golay, "Complementary series", *IEEE Trans. Inf. Theory*, vol. IT-7, no. 2, pp. 82-87, 1961.

[13] M. Hein, W. Dur, J. Eisert, R. Raussendorf, M. Van den Nest, H.-J. Briegel, "Entanglement in Graph States and its Applications", International School of Physics Enrico Fermi (Varenna, Italy), Quantum computers, algorithms and chaos 162 (Eds.: P. Zoller, G. Casati, D. Shepelyansky, G. Benenti), 2006. arXiv:0602096 [quant-ph].

[14] I. D. Ivanović, "Geometrical description of quantal state determination", *J. Phys. A*, 14(12), 3241–3245, 1981.

[15] J. Jedwab, M. G. Parker, "Golay Complementary Array Pairs", *Designs, Codes and Cryptography*, 44, pp. 209–216, July 2007.

[16] F. R. Kschischang, B. J. Frey, H-A. Loeliger, "Factor Graphs and the Sum-Product Algorithm", *IEEE Trans. Inform. Theory*, vol. 47, no. 2, Feb. 2001.

[17] S. Matsufuji, R. Shigemitsu, Y. Tanada, N. Kuroyanagi, "Construction of Complementary Arrays", Proc. of Sympotic'04, 78–81, 2004.

[18] The On-Line Encyclopedia of Integer Sequences, `http://oeis.org/`, 2013.

[19] M. G. Parker and C. Tellambura, "Golay-Davis-Jedwab Complementary Sequences and Rudin-Shapiro Constructions", Int. Symp. Information Theory, Sorrento, p. 302, June 25–30, 2000.

[20] M. G. Parker and C. Tellambura, "A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio", *Reports in Informatics*, University of Bergen, Report No 242, ISSN 0333–3590, February 2003. `http://www.ii.uib.no/~matthew/ConstructReport.pdf`

[21] M. G. Parker, C. Riera, "Generalised complementary arrays", *Lecture Notes in Computer Science*, LNCS 7089, Springer, 2011.

[22] K. G. Paterson, "Generalized Reed-Muller codes and power control in OFDM modulation", *IEEE Trans. Inform. Theory*, 46:104–120, 2000.

[23] C. Riera, S. Jacob, M. G. Parker, "From Graph States to Two-Graph States", Designs, Codes and Cryptography, vol. 48, 2, August, 2008. arXiv:0801.4754 [quant-ph].

[24] M. B. Ruskai, "Some Connections between Frames, Mutually Unbiased Bases, and POVM's in Quantum Information Theory", *Acta Applicandae Mathematicae*, Volume 108, Issue 3, pp 709–719, December 2009.

[25] D. Sarwate, "Meeting the Welch bound with equality", in Proc. SETA'98 Sequences Their Appl. London, U.K.: Springer, pp. 79–102, 1999.

[26] K-U. Schmidt, "On cosets of the generalized first-order Reed-Muller code with low PMEPR", *IEEE Trans. Inf. Theory,* vol. 52, no. 7, pp. 3220–3232, Jul. 2006.

[27] K-U. Schmidt, "Complementary sets, generalized Reed-Muller codes, and power control for OFDM", *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 808–814, Feb. 2007.

[28] J. Schwinger, "Unitary Operator Bases", Harvard University, 1960.

[29] H. S. Shapiro, "Extremal problems for polynomials and power series", Master's thesis, Mass. Inst. of Technology, 1951.

[30] N. Suehiro, M. Hatori, "N-shift cross-orthogonal sequences", *IEEE Trans. Inform. Theory*, vol. IT-34, no. 1, pp. 143–146, Jan. 1988.

[31] Z. Wang, M. G. Parker, G. Gong, G. Wu, "On the PMEPR of binary Golay sequences of length 2^n", submitted, June 2013.

[32] L. Welch, "Lower bounds on the maximum cross correlation of signals", *IEEE Trans. Inform. Theory*, vol. 20, no. 3, pp. 397–399, May 1974.

[33] H. S. Wilf, Generatingfunctionology, 2nd edn., Academic Press, NY, 1994.